CLAIMS

1. A method of propagating rights management (RM) protection to an email and to an attachment of the email, the attachment comprising an RM-protectable document, the method comprising:

authoring the email with the RM-protectable attachment;

generating a content key (KD);

generating a bind ID;

firstly applying RM protection to the RM-protectable attachment of the email based on the generated (KD) and the generated bind ID;

attaching the RM-protected attachment to the email;

secondly applying RM protection to the email with the attached RM-protected attachment based on the generated (KD) and the generated bind ID;

wherein the RM-protected email and the RM-protected attachment thereof share the generated (KD) and the generated bind ID such that a license obtained for the RM-protected email and having therein the generated bind ID and the generated (KD) can be applied to render the RM-protected email and also the RM-protected attachment thereof.

2. The method of claim 1 further comprising:

protecting (KD) to an RM server so that all requests for a license corresponding to the item are directed to such RM server; and

generating rights data including the protected (KD) and the generated bind ID and setting forth each entity that has rights with respect to the RM-protected email and the RM-protected attachment thereof and for each such entity a description of such rights; and

wherein applying RM protection to each item comprises:

encrypting the item with (KD) to form (KD(item)); and

attaching the rights data to the corresponding (KD(item)) to form a package containing the item in an RM-protected form, whereby the signed rights data from the package for any item may be employed to obtain the license for the RM-protected email and the RM-protected attachment thereof, such license thus including the bind ID of the signed rights data and being bound to the RM-protected email and the RM-protected attachment thereby.

3. The method of claim 2 further comprising submitting the generated rights data for signing and receiving signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any changes to the signed rights data will cause the signature to fail to verify, and wherein attaching the rights data comprises attaching the signed rights data.

4. The method of claim 3 wherein submitting the rights data for signing comprises submitting the rights data to the RM server for signing.

5. The method of claim 2 wherein protecting (KD) comprises encrypting (KD) with a public key of the RM server to result in (PU-RM(KD)) such that only the RM server with a corresponding private key (PR-RM) can decrypt (PU-RM(KD)) to reveal (KD).

6. The method of claim 2 wherein attaching the rights data comprises concatenating the signed rights data with the corresponding (KD(item)) to form a package containing the item in an RM-protected form.

7. An email having an attachment, the email and the attachment being rights management (RM) protected, the attachment of the email being RM-protected based on a particular content key (KD) and a particular bind ID, the email with the RM-protected attachment itself being RM-protected based on the particular content key (KD) and the particular bind ID, wherein the RM-protected email with the RM-protected attachment therein share the particular (KD) and the particular bind ID such that a license obtained for the RM-protected email and

having therein the generated bind ID and the generated (KD) can be applied to render the RM-protected email and also the RM-protected attachment therein.

8. The email of claim 1 wherein the RM protection for each item comprises the item being encrypted with (KD) to form (KD(item)) and having attached thereto common rights data to form a package containing the item in an RM-protected form, the common rights data including the particular bind ID and the particular (KD) protected to an RM server so that all requests for a license corresponding to the item are directed to such RM server, and setting forth each entity that has rights with respect to the RM-protected email and the RM-protected attachment thereof and for each such entity a description of such rights, whereby the rights data from the package for any item may be employed to obtain the license for the RM-protected email and the RM-protected attachment therein, such license thus including the bind ID of the signed rights data and being bound to the RM-protected email and the RM-protected attachment thereby.

9. The email of claim 8 wherein the common rights data comprises rights data submitted for signing and received as signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any changes to the signed rights data will cause the signature to fail to verify.

10. The email of claim 9 wherein the rights data is submitted to the RM server for signing.

11. The email of claim 8 wherein (KD) protected comprises (KD) encrypted with a public key of the RM server to result in (PU-RM(KD)) such that only the RM server with a corresponding private key (PR-RM) can decrypt (PU-RM(KD)) to reveal (KD).

12. The email of claim 8 wherein the rights data is concatenated with the corresponding (KD(item)) to form a package containing the item in an RM-protected form.

13. A computer-readable medium having stored thereon computer-executable instructions for performing a method of propagating rights management (RM) protection to an email and to an attachment of the email, the attachment comprising an RM-protectable document, the method comprising:

authoring the email with the RM-protectable attachment;

generating a content key (KD);

generating a bind ID;

firstly applying RM protection to the RM-protectable attachment of the email based on the generated (KD) and the generated bind ID;

attaching the RM-protected attachment to the email;

secondly applying RM protection to the email with the attached RM-protected attachment based on the generated (KD) and the generated bind ID;

wherein the RM-protected email and the RM-protected attachment thereof share the generated (KD) and the generated bind ID such that a license obtained for the RM-protected email and having therein the generated bind ID and the generated (KD) can be applied to render the RM-protected email and also the RM-protected attachment thereof.

14. The medium of claim 13 wherein the method further comprises:

protecting (KD) to an RM server so that all requests for a license corresponding to the item are directed to such RM server; and

generating rights data including the protected (KD) and the generated bind ID and setting forth each entity that has rights with respect to the RM-protected email and the RM-protected attachment thereof and for each such entity a description of such rights; and

wherein applying RM protection to each item comprises:

encrypting the item with (KD) to form (KD(item)); and

attaching the rights data to the corresponding (KD(item)) to form a package containing the item in an RM-protected form, whereby the signed

rights data from the package for any item may be employed to obtain the license for the RM-protected email and the RM-protected attachment thereof, such license thus including the bind ID of the signed rights data and being bound to the RM-protected email and the RM-protected attachment thereby.

15. The medium of claim 14 wherein the method further comprises submitting the generated rights data for signing and receiving signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any changes to the signed rights data will cause the signature to fail to verify, and wherein attaching the rights data comprises attaching the signed rights data.

16. The medium of claim 15 wherein submitting the rights data for signing comprises submitting the rights data to the RM server for signing.

17. The medium of claim 14 wherein protecting (KD) comprises encrypting (KD) with a public key of the RM server to result in (PU-RM(KD)) such that only the RM server with a corresponding private key (PR-RM) can decrypt (PU-RM(KD)) to reveal (KD).

18. The medium of claim 14 wherein attaching the rights data comprises concatenating the signed rights data with the corresponding (KD(item)) to form a package containing the item in an RM-protected form.

19. A computer-readable medium having stored thereon a data structure comprising an email having an attachment, the email and the attachment being rights management (RM) protected, the attachment of the email being RM-protected based on a particular content key (KD) and a particular bind ID, the email with the RM-protected attachment itself being RM-protected based on the particular content key (KD) and the particular bind ID, wherein the RM-protected email with the RM-protected attachment therein share the particular (KD) and the particular bind ID such that a license obtained for the RM-protected email and

having therein the generated bind ID and the generated (KD) can be applied to render the RM-protected email and also the RM-protected attachment therein.

20. The medium of claim 19 wherein the RM protection for each item comprises the item being encrypted with (KD) to form (KD(item)) and having attached thereto common rights data to form a package containing the item in an RM-protected form, the common rights data including the particular bind ID and the particular (KD) protected to an RM server so that all requests for a license corresponding to the item are directed to such RM server, and setting forth each entity that has rights with respect to the RM-protected email and the RM-protected attachment thereof and for each such entity a description of such rights, whereby the rights data from the package for any item may be employed to obtain the license for the RM-protected email and the RM-protected attachment therein, such license thus including the bind ID of the signed rights data and being bound to the RM-protected email and the RM-protected attachment thereby.

21. The medium of claim 20 wherein the common rights data comprises rights data submitted for signing and received as signed rights data based thereon, whereby the signed rights data is tamper-resistant in that any changes to the signed rights data will cause the signature to fail to verify.

22. The medium of claim 21 wherein the rights data is submitted to the RM server for signing.

23. The medium of claim 20 wherein (KD) protected comprises (KD) encrypted with a public key of the RM server to result in (PU-RM(KD)) such that only the RM server with a corresponding private key (PR-RM) can decrypt (PU-RM(KD)) to reveal (KD).

24. The medium of claim 20 wherein the rights data is concatenated with the corresponding (KD(item)) to form a package containing the item in an RM-protected form.